PATENT ABSTRACTS OF JAPAN

(11)Publication number : 05-040537
(43)Date of publication of application : 19.02.1993

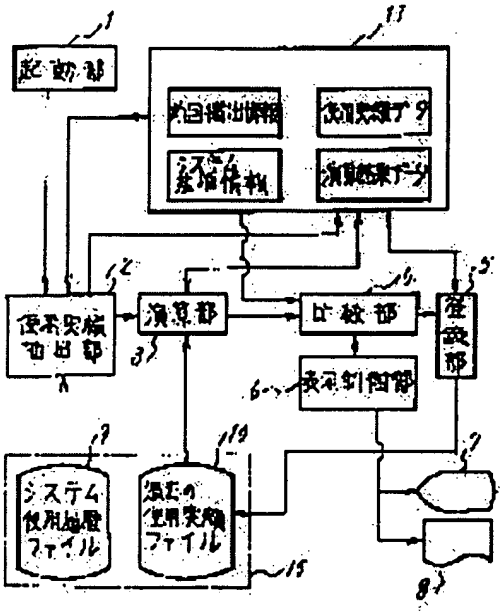
(51)Int.Cl. G06F 1/00
G06F 11/34

(21)Application number : 03-000403
(22)Date of filing : 08.01.1991

(71)Applicant : NEC CORP
(72)Inventor : TAKEUCHI ISAMU

(54) DETECTING DEVICE FOR ILLEGAL USE OF SYSTEM FOR INFORMATION PROCESSING SYSTEM

(57)Abstract:
PURPOSE: To timely and correctly detect the illegal use of an information processing system.
CONSTITUTION: The system use history information of the information processing system is stored in a storage part 15. A starting part 1 sends a start signal for checking periodically the using state of the information processing system. A used result extracting part 2 receives the start signal, and extracts the latest used result data from system use history information. An arithmetic part 3 executes the arithmetic operation of data to be used for checking the using state by using the latest used result data and the used result data in the past. A comparing part 4 compares the latest used result data, system reference information and arithmetic result data, and detects the illegal use of the system. A registering part 5 registers the latest used result data extracted newly in a past used result file 10 as the used result data in the past.



LEGAL STATUS

[Date of request for examination]

[Date of sending the examiner's decision of rejection]

[Kind of final disposal of application other than the examiner's decision of rejection or application converted registration]

[Date of final disposal for application]

[Patent number]

[Date of registration]

[Number of appeal against examiner's decision of rejection]

[Date of requesting appeal against examiner's decision of rejection]

[Date of extinction of right]

(19)日本国特許庁（ＪＰ）　(12)公開特許公報（Ａ）　(11)特許出願公開番号

特開平5－40537

(43)公開日　平成５年(1993)２月19日

(51)Int.Cl.[5]		識別記号	庁内整理番号	ＦＩ	技術表示箇所
Ｇ０６Ｆ	1/00	３７０　Ｅ	7927－5Ｂ		
	11/34	Ｃ	8725－5Ｂ		

審査請求　未請求　請求項の数１(全　４　頁)

(21)出願番号　特願平3－403

(22)出願日　平成３年(1991)１月８日

(71)出願人　000004237
日本電気株式会社
東京都港区芝五丁目７番１号

(72)発明者　竹内　勇
東京都港区芝五丁目７番１号日本電気株式会社内

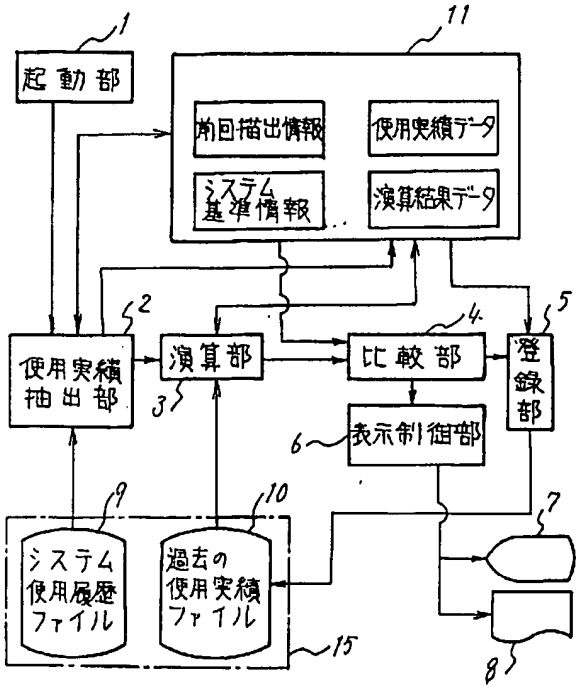
(74)代理人　弁理士　内原　晋

(54)【発明の名称】　情報処理システムのシステム不正使用検出装置

(57)【要約】

【構成】記憶部１５は、情報処理システムのシステム使用履歴情報が格納されている。起動部１は、情報処理システムの使用状況のチェックを定期的に行うための起動信号を送出する。使用実績抽出部２は、起動信号を受信し、システム使用履歴情報から、最新の使用実績データを抽出する。演算部３は、最新の使用実績データと、過去の使用実績データとを用いて使用状況のチェックのために使用するデータの演算を行う。比較部４は、最新の使用実績データ、システム基準情報、及び演算結果データを比較してシステム不正使用を検出する。登録部５は、新しく抽出された最新の使用実績データを、過去の使用実績データとして過去の使用実績ファイル１０に登録する。

【効果】情報処理システムの不正使用を誤りなくタイムリーに検出することができる。



1

【特許請求の範囲】

【請求項1】　情報処理システムの不正使用をチェックする情報処理システムのシステム不正使用検出装置であって、

（A）前記情報処理システムについてのシステム使用履歴情報を有したシステム使用履歴ファイルと、一度チェックされた過去の使用実績データを有した過去の使用実績ファイルとを格納している記憶部、

（B）タイマ機能を有し、使用状況のチェックを定期的に行うための起動信号を送出する起動部、

（C）前記起動信号を受信し、前記システム使用履歴情報から、前回のチェック後に記録された最新のシステム使用履歴情報を最新の使用実績データとして抽出する使用実績抽出部、

（D）前記最新の使用実績データと、前記過去の使用実績ファイルから読み出した過去の使用実績データとを用いて使用状況のチェックのために使用するデータの演算を行う演算部、

（E）前記システム使用履歴情報から前回使用実績データを抽出した時刻を含む情報と、使用状況のチェックを行うためにシステムで規定しているシステム基準情報と、前記最新の使用実績データと、前記演算部で算出された値である演算結果データとを記憶する主記憶部、

（F）前記最新の使用実績データ、システムで規定しているシステム基準情報、及び前記演算部で算出された演算結果データを比較してシステム不正使用を検出する比較部、

（G）前記最新の使用実績データを過去の使用実績データとして前記過去の使用実績ファイルに登録する登録部、

（H）不正使用と判定した使用実績データを編集し出力する表示制御部、

を備えたことを特徴とする情報処理システムのシステム不正使用検出装置。

【発明の詳細な説明】

【0001】

【産業上の利用分野】本発明は、情報処理システムにおけるシステムの不正使用の検出に用いられる情報処理システムのシステム不正使用検出装置に関する。

【0002】

【従来の技術】従来、バッチシステム，オンラインシステム等の情報処理システムの不正使用、あるいはファイル，端末装置等の資源に対する不正アクセスについては、そのシステムが有する資源使用者管理機能により、資源使用履歴情報を記録して、システム管理者が、通常これらの情報を編集・出力し、システム及び資源に対する不正なアクセス，データの破壊，機密漏洩等の不正な行為が行われようとしたか否かを調べることにより、システム不正使用の監視を行っている。

【0003】

2

【発明が解決しようとする課題】上述した従来のシステム不正使用を監視する方法では、システムで記録しているシステム使用履歴情報をもとに、システム管理者がチェックを行うため、一定の検証規準が作成されていても、チェックを行うシステム管理者の思い違い等で誤ったチェックを行う恐れがあり、さらにシステムの不正使用を防止するため、細かなチェックを頻繁に行う場合は、検証作業が大きな負担となり、不正使用が行われたことをタイムリーに発見することができない場合が多かった。

【0004】また、システムを不正に使用しようとする人間が、使用が禁止されているファイル，システムへのアクセスを行うために、他の正規の使用者のパスワード等を推測しては不正な入力を繰返した痕跡は、入力の記録をチェックすれば比較的容易に確認できるが、一回で不正なアクセスに成功した場合、あるいは使用者がシステムで定められている使用規則，範囲を逸脱して使用した場合については、不正使用を疑うだけの明確な記録が残らない場合が多く、その検出は困難であるという欠点を有している。

【0005】本発明の目的は、不正使用者を誤りなくタイムリーに発見することができる情報処理システムのシステム不正使用検出装置を提供することにある。

【0006】

【課題を解決するための手段】本発明の情報処理システムのシステム不正使用検出装置は、情報処理システムの不正使用をチェックするシステム不正使用検出装置であって、（A）前記情報処理システムについてのシステム使用履歴情報を有したシステム使用履歴ファイルと、一度チェックされた過去の使用実績データを有した過去の使用実績ファイルとを格納している記憶部、（B）タイマ機能を有し、使用状況のチェックを定期的に行うための起動信号を送出する起動部、（C）前記起動信号を受信し、前記システム使用履歴情報から、前回のチェック後に記録された最新のシステム使用履歴情報を最新の使用実績データとして抽出する使用実績抽出部、（D）前記最新の使用実績データと、前記過去の使用実績ファイルから読み出した過去の使用実績データとを用いて使用状況のチェックのために使用するデータの演算を行う演算部、（E）前記システム使用履歴情報から前回使用実績データを抽出した時刻を含む情報と、使用状況のチェックを行うためにシステムで規定しているシステム基準情報と、前記最新の使用実績データと、前記演算部で算出された値である演算結果データとを記憶する主記憶部、（F）前記最新の使用実績データ、システムで規定しているシステム基準情報、及び前記演算部で算出された演算結果データを比較してシステム不正使用を検出する比較部、（G）前記最新の使用実績データを過去の使用実績データとして前記過去の使用実績ファイルに登録する登録部、（H）不正使用と判定した使用実績データ

3

を編集し出力する表示制御部、を備えて構成されている。

【０００７】

【実施例】次に、本発明の実施例について図面を参照して説明する。

【０００８】図１は本発明の情報処理システムのシステム不正使用検出装置の一実施例を示すブロック図である。

【０００９】本実施例の情報処理システムのシステム不正使用検出装置は、図１に示すように、情報処理システムについてのシステム使用履歴情報を有したシステム使用履歴ファイル９と、一度チェックされた過去の使用実績データを有した過去の使用実績ファイル１０とを格納している記憶部１５、タイマ機能を有し、使用状況のチェックを定期的に行うための起動信号を送出する起動部１、起動信号を受信し、システム使用履歴情報から、前回のチェック後に記録された最新のシステム使用履歴情報を最新の使用実績データとして抽出する使用実績抽出部２、最新の使用実績データと、過去の使用実績ファイル１０から読み出した過去の使用実績データとを用いて使用状況のチェックのために使用するデータの演算を行う演算部３、システム使用履歴情報から前回使用実績データを抽出した時刻を含む情報と、使用状況のチェックを行うためにシステムで規定しているシステム基準情報と、最新の使用実績データと、演算部３で算出された値である演算結果データとを記憶する主記憶部１１、最新の使用実績データ、システムで規定しているシステム基準情報、及び演算部３で算出された演算結果データを比較してシステム不正使用を検出する比較部４、最新の使用実績データを過去の使用実績データとして過去の使用実績ファイル１０に登録する登録部５、不正使用と判定した使用実績データを編集し出力する表示制御部６、ディスプレイ７、プリンタ８から構成されている。

【００１０】次に、動作を説明する。

【００１１】図１において、起動部１は、システム不正使用のチェックを自動的に定期的に行うため、タイマにより定期的に信号を使用実績抽出部２へ送出する。使用実績抽出部２は、起動部１からの信号を受信すると、システム使用履歴ファイル９から、前回の抽出の後に記録されたシステム使用履歴情報である最新のシステム使用実績データを抽出し、主記憶部１１へ使用実績データとして登録する。そして、主記憶部１１へ抽出したデータの登録が完了すると、主記憶部１１に記録されている、

4

前回の使用実績データが抽出された時刻等のデータを、新しく使用実績データが抽出された時刻等のデータに更新する。

【００１２】次に、演算部３が、主記憶部１１に登録されている最新の使用実績データと過去の使用実績ファイル１０に登録されているデータとを用い、最新の使用実績データと、その使用者の過去の使用実績平均データとを比較して単位時間当りのＣＰＵ使用時間、あるいは一定期間でのシステム接続回数の差等のデータを求め、これを主記憶部１１へ演算結果データとして登録する。

【００１３】次に、比較部４が、主記憶部１１に登録されている使用実績データ、演算結果データ、及びシステム基準情報（許容範囲値等）との比較を行い、使用実績データの中から不正使用を示しているデータを選別する。選別された不正使用を示しているデータは、表示制御部６によりディスプレイ７及びプリンタ８へ出力される。そして、抽出された最新の使用実績データは、登録部５により過去の使用実績ファイル１０に登録される。

【００１４】

【発明の効果】以上説明したように、本発明の情報処理システムのシステム不正使用検出装置は、過去の使用実績データとシステム不正使用を判定するシステム基準情報を登録し、これら情報と現在のシステム使用情報とを定期的に比較することにより、不正使用を誤りなくタイムリーに検出することができるという効果を有している。

【図面の簡単な説明】

【図１】本発明の情報処理システムのシステム不正使用検出装置の一実施例を示すブロック図である。

【符号の説明】

１　起動部
２　使用実績抽出部
３　演算部
４　比較部
５　登録部
６　表示制御部
７　ディスプレイ
８　プリンタ
９　システム使用履歴ファイル
１０　過去の使用実績ファイル
１１　主記憶部
１５　記憶部

【図１】